



University of Massachusetts
Amherst

Controller's Office
405 Goodell Building
140 Hicks Way
Amherst, MA 01003-9334

phone: 413.545.1675
fax: 413.545.6088
email: amangels@admin.umass.edu

March 20, 2008

Amherst Campus Credit Card Information Policy

1. Accepting Credit Card Payments

- a. Schools and departments planning to accept debit and credit cards must first contact the Amherst campus E-Commerce representative. The campus E-Commerce representative must approve any decisions to accept debit and credit cards or other electronic forms of cash receipts.
- b. The Amherst campus E-Commerce representative and Amherst campus bursar will work with departments to provide the necessary guidance in the areas of PCI DSS (Payment Card Industry Data Security Standard) Compliance, internal controls, deposit techniques and reconciliation procedures.
- c. Bank accounts and debit and credit card accounts may only be opened by the University Treasurer's Office. "Paypal" accounts and other web-based payment mechanisms are not permitted for conducting university business unless approved by the Amherst E-commerce representative and Treasurer's office.
- d. CyberSource has been identified as the third party vendor of choice for all web-based e-commerce activity. See below for use of alternative 3rd party systems.
- e. All broken and discontinued POS terminals must be returned to the University Treasurer's office in a secure manner.

2. Storing Credit Card Data Electronically

- a. Departments are prohibited from storing sensitive cardholder data including the 16 digit credit card number, the CVV2 number (3 digit value printed on the signature panel of payment card) or PIN data on any computer, database, network or file without approval from the University's Treasurer's Office, and Amherst Campus Controller. Storing sensitive cardholder data electronically exposes the campus to credit card identity theft with substantial penalties for lost or stolen data.

- b. Requests to electronically store sensitive cardholder data must be signed by the Dean and Department Head. Schools and departments will be responsible for all fines and penalties relating to loss or theft of credit card data.
- c. Departments storing credit card data electronically must submit to and comply with PCI compliance standards.

3. Storing Credit Card Data on Paper Forms or Reports

- a. Departments at times receive credit card information filled out on order forms, faxes, etc. as part of conducting university business. In addition, sensitive credit card data may be printed on daily logs, reports and receipts. Departments should redact any sensitive cardholder data printed on paper by blacking out or detaching and shredding the information. See records retention policy below.
- b. All systems that print out the full 16 character credit card number on any receipt or report should be upgraded to only print the last four digits of the card number. This includes all university issued credit card terminals.
- c. Card information should not be communicated via unencrypted electronic communications (e.g., email, instant messaging). Merchants shall not email/instant message card information. If a merchant contacts a customer via email/instant message all card information must be deleted prior to the message being sent. Under no circumstances should departments take a photocopy of a customer's debit or credit card.
- d. After a transaction has been authorized, access to card data should be limited to staff with a sound business need to access this information. All hardcopy Cardholder information should be securely stored or destroyed. Departments needing to retain sensitive cardholder data beyond transaction authorization must submit a request to the Amherst campus controller indicating the following:
 - 1. Explanation of the business need to retain credit card data
 - 2. Length of time data will be retained, i.e. X days beyond transaction date
 - 3. Method to secure printed credit card data which must include suitably locked file cabinets etc.
 - 4. Description of who can access stored information
 - 5. Method by which data will be destroyed

4. Record Retention and Disposal Guidelines for Credit Card Transactions

- a. Departments must retain the invoice or other relevant information pertaining to a sales transaction for 3 years after the transaction date.

- b. After the retention period has lapsed, departments must dispose of records via shredding or other suitable means to ensure sensitive customer data is not compromised.
- c. Archived documents containing full payment card numbers should be identified, securely stored in locked file cabinets and/or rooms, and properly disposed of after the retention period has lapsed.

5. Third Party Applications

- a. CyberSource has been identified as the third party vendor of choice for all web-based e-commerce activity and compliance with PCI standards is handled by the President's Office
- b. The use of any other 3rd party credit card processor must be approved by the E-commerce representative and Treasurer's office
- c. All third party credit card processing vendors are subject to PCI compliance standards including quarterly network scans by approved vendors, completion of annual self assessment questionnaires, listing on VISA's list of compliant service providers and other compliance requirements.
- d. All new contracts with third party or outside vendors must contain language requiring the vendor be PCI DSS Compliant and will remain PCI DSS - Compliant.
- e. Schools and departments will be responsible for all fines and penalties relating to loss or theft of credit card data from third party vendors.

Questions concerning these policies may be forwarded to the Controller's office at 545-0806.